

On Lower Bound of Worst Case Error Probability for Quantum Fingerprinting with Shared Entanglement

Xin Li, Tian Liu, Han Peng*, Hongtao Sun, Jiaqi Zhu

School of EECS, Peking University, P.R.China

February 1, 2008

Abstract

This paper discusses properties of quantum fingerprinting with shared entanglement. Under certain restriction of final measurement, a relation is given between unitary operations of two parties. Then, by reducing to spherical coding problem, this paper gives a lower bound of worst case error probability for quantum fingerprinting with shared entanglement, showing a relation between worst case error probability and the amount of entanglement(measured by Schmidt number).

Key Words: quantum information, quantum fingerprinting, worst case error probability, quantum entanglement, Welch bound

1 introduction

Fingerprinting is a useful tool to determine whether two copies of message are identical, especially for large and distributed data where both parties have to communicate to accomplish this task. Instead of comparing original messages, it is enough to compare short messages called "fingerprints" of them if some manageable error probability is allowed. The goal of fingerprinting is to reduce the amount of communication while maintain acceptable error probability.

The notion of fingerprinting first appeared in communication complexity ([1]) research where the amount of communication is calculated and local

*Corresponding author, penghan@tcs.pku.edu.cn

computational complexity ignored. Discussion in this paper is based on SMP (Simultaneous Message Passing) model introduced by Yao in [2], where 3 distributed parties, say Alice, Bob, and Roger, are involved. They cooperate to compute some function $f(x, y)$, but Alice holds x , Bob holds y . Mutual communication is not allowed between Alice and Bob, but they can each send one message to Roger, who will then compute $f(x, y)$ based on received messages. This problem can be trivially solved if Alice and Bob send entire messages to Roger, but the question is: what error probability can be achieved if they transfer shorter messages? When $f(x, y)$ is defined as

$$f(x, y) = \begin{cases} 1 & \text{if } x = y \\ 0 & \text{else} \end{cases} \quad (1)$$

the messages sent by Alice and Bob are called *fingerprints* of x and y , respectively. When qubits are used as fingerprints, they are called quantum fingerprints.

Quantum fingerprinting was introduced in [3], where the author showed that $O(\log n)$ qubits of communication suffice to determine the equality of two n -bit strings with bounded error probability. On the other hand, however, Ambainis proved in [4] that $\Theta(\sqrt{n})$ classical bits are necessary for the same problem, showing an exponential gap. Later in [5] Scott et. al. analyzed the relation between worst case error probability and actual number of transferred qubits, giving a lower bound on achievable worst case error probability.

However, the first quantum fingerprinting scheme in [3] does not consider shared *a priori* entanglement between Alice and Bob. In [6], Horn et. al. discussed such case. Since shared entanglement can easily be used as shared randomness, the authors also made comparison between classical fingerprinting with shared randomness and quantum fingerprinting with shared entanglement.

This paper can be seen as an extension of [5] onto the shared entanglement case of quantum fingerprinting. We discuss properties of shared entanglement quantum fingerprinting under certain restriction of measurement, and give a relation between lower bound of achievable worst case error probability and amount of entanglement(measured by Schmidt number).

2 Communication Model

This section will describe the communication model of shared-entanglement quantum fingerprinting used in this paper. First introduce the definition of one-sided error.

Definition 1 A fingerprinting scheme is one-sided error if for any $x = y \in M$, Roger always produces correct answer.

Definition 2 A quantum fingerprinting scheme with shared entanglement operates as follows. First, Alice and Bob receive messages $x, y \in M$, respectively. Then each of them performs certain unitary operation on their own part of shared entanglement, and sends these qubits to Roger. On receiving qubits from both parties, Roger performs a measurement and produces an output based on result. Such a scheme is characterized by 4 components:

- Shared entanglement $|E\rangle$, where we suppose the Schmidt decomposition of $|E\rangle$ is

$$|E\rangle = \sum_{k=1}^{N_s} \lambda_k |k\rangle_A |k\rangle_B$$

λ_k being the Schmidt coefficients and N_s the Schmidt number.

- Alice's unitary operation set $\{U_x\}_{x \in M}$, where she applies U_x on her shared entanglement upon receiving message x .
- Bob's unitary operation set $\{V_x\}_{x \in M}$, where he applies V_x on his shared entanglement upon receiving message x .
- Roger's measurement and decision strategy, which is restricted due to the following reasons:
 - The scheme has only one-sided error, so that Roger's decision strategy must be deterministic.
 - Roger performs such kind of POVM on received qubits:

$$\{|\alpha\rangle\langle\alpha|, I - |\alpha\rangle\langle\alpha|\}$$

and announces $x = y$ if the measurement result corresponds to $|\alpha\rangle\langle\alpha|$.

Define worst case error probability as

Definition 3

$$P_{wce} = \max_{x,y \in M} P\{x \neq y, \text{ but Roger announces } x = y\}$$

3 Relation of unitary operations

As described in previous section, the Schmidt decomposition of shared entanglement between Alice and Bob is

$$|E\rangle = \sum_{i=1}^{N_s} \lambda_i |i\rangle_A |i\rangle_B$$

where $|i\rangle_A, i = 1, 2, \dots, N_s$, are a group of orthonormal vectors in Alice's subsystem, and $|i\rangle_B, i = 1, 2, \dots, N_s$, are a group of orthonormal vectors in Bob's subsystem. Extend both groups to be orthonormal bases of the two subsystems, respectively, and denote them by $|i\rangle_A, i = 1, 2, \dots, n$, and $|j\rangle_B, j = 1, 2, \dots, n$.

In Roger's POVM, let

$$|\alpha\rangle = \sum_{i,j=1}^n \alpha_{i,j} |i\rangle_A |j\rangle_B$$

where $\sum_{i,j=1}^n |\alpha_{i,j}|^2 = 1$

The following lemma is easily found in linear algebra textbooks.

Lemma 1 ([7]) *Denote by L_V^n the set of linear operators on \mathbb{C}^n , and define function $(\cdot, \cdot) : L_V^n \times L_V^n \rightarrow \mathbb{C}$ as*

$$(A, B) \equiv \text{tr}(A^\dagger B)$$

then (\cdot, \cdot) is an inner product on L_V^n , which is then an n^2 -dimension Hilbert space.

The following theorem shows the relation between unitary operations of Alice and Bob.

Theorem 1 $\forall x \in M, U_x K V_x^T = S$, where S is constant with respect to a global constant $e^{i\theta}$ and is independent with x . K depends only on the Schmidt decomposition of $|E\rangle$.

Proof Suppose Alice and Bob receive messages x and y , respectively, then Roger receives from them the following state

$$U_x \otimes V_y \sum_{k=1}^{N_s} \lambda_k |k\rangle_A |k\rangle_B$$

Since Roger uses POVM $\{|\alpha\rangle\langle\alpha|, I - |\alpha\rangle\langle\alpha|\}$, measurement result corresponding to $|\alpha\rangle\langle\alpha|$ appears with probability

$$q = \left| \langle \alpha | U_x \otimes V_y \sum_{k=1}^{N_s} \lambda_k |k\rangle_A |k\rangle_B \right|^2$$

then we have

$$\begin{aligned} q &= \left| \sum_{i,j=1}^n \alpha_{ij}^* \langle i | A \langle j | B U_x \otimes V_y \sum_{k=1}^{N_s} \lambda_k |k\rangle_A |k\rangle_B \right|^2 \\ &= \left| \sum_{i,j=1}^n \sum_{k=1}^{N_s} \alpha_{ij}^* \lambda_k \langle i | A U_x |k\rangle_A \langle k | B V_y^T |j\rangle_B \right|^2 \\ &= \left| \sum_{i,j=1}^n \alpha_{ij}^* \langle i | A K V_y^T |j\rangle_B \right|^2 \\ &= \left| \text{tr}(A^\dagger U_x K V_y^T) \right|^2 \end{aligned}$$

where $K = \sum_{k=1}^{N_s} |k\rangle\langle k|$. Let $S(x, y) = U_x K V_y^T$, then

$$q = \left| \text{tr}(A^\dagger S(x, y)) \right|^2$$

Recall that we require this scheme has single-sided error probability, which means that when $x = y$ Roger must have $|q| = 1$, that is

$$\left| \text{tr}(A^\dagger S(x, x)) \right| = 1 \quad (2)$$

According to Lemma 1, Eq (2) is equivalent to the condition that the projection of vector $S(x, y) \in L_V^n$ onto vector $A^\dagger \in L_V^n$ has length 1. On the other hand, A^\dagger itself has length 1, and $S(x, y)$ also has length 1:

$$\begin{aligned} |S(x, y)|^2 &= \text{tr}((S(x, y))^\dagger S(x, y)) \\ &= \text{tr}((U_x K V_y^T)^\dagger (U_x K V_y^T)) \\ &= \text{tr}(V_y^* K^\dagger K V_y^T) \\ &= \text{tr}(V_y K^\dagger K V_y^T) \\ &= 1 \end{aligned}$$

Therefore, in order to satisfy (2), it is necessary that

$$A = e^{i\theta} S(x, x) \quad (3)$$

where θ is an arbitrary constant, i the imaginary unit. Because entries in A are completely determined by $|\alpha\rangle$ in Roger's POVM, which should be constant, we have

$$e^{i\theta} U_x K V_x^T = \text{const} \quad (4)$$

□

Note that when $N_s = n$ (the dimension of each subsystem), K has full rank and K^{-1} exists, then V_x is determined by U_x with respect to a unit global coefficient, and vice versa

$$V_x = (e^{-i\theta} K^{-1} U_x^\dagger A)^T$$

4 Lower bound of worst case error probability

Theorem 2 $P_{wce} \geq \frac{m - N_s^2}{N_s^2(m-1)}$

Proof q is error probability when $x \neq y$

$$\begin{aligned} q &= \left| \text{tr}(A^\dagger S(x, y)) \right|^2 \\ &= \left| \text{tr}(S(x, x) S(x, y)) \right|^2 \\ &= \left| \text{tr}((U_x K V_x^T)^\dagger U_x K V_y^T) \right|^2 \\ &= \left| \text{tr}(V_x^* K^\dagger K V_y^T) \right|^2 \\ &= \left| \text{tr}(V_y K K^\dagger V_x^\dagger) \right|^2 \end{aligned}$$

then

$$P_{wce} = \min_{|V|=m} \max_{V_x, V_y \in V, V_x \neq V_y} \left| \text{tr}(V_y K K^\dagger V_x^\dagger) \right|^2 \quad (5)$$

Let $W_x = V_x K$, $W_y = V_y K$, the above equation can be reformulated as

$$P_{wce} = \min_{|V|=m} \max_{V_x, V_y \in V} \left| \text{tr}(W_y W_x^\dagger) \right|^2$$

If $N_s = n$, K has full rank, W_x and W_y are linear operators in L_V^n . According to Lemma 1, the above min-max problem can be seen as a spherical coding problem, by Welch Bound([8])

$$P_{wce} \geq \frac{m - N_s^2}{N_s^2(m-1)}$$

this proves the $N_s = n$ case of Theorem 2. Now we focus on the case of $N_s < n$.

Let $J = \sum_{i=1}^{N_s} \sqrt{\lambda_i} |i\rangle_A \langle i|_B$, then (4) can be reformulated as (where we omit global coefficient $e^{i\theta}$)

$$U_x J (V_x J)^T = \text{const}$$

Choose an arbitrary basis and write U_x as a matrix. Because U_x is unitary, n columns of this matrix represent a group of orthonormal vectors on \mathbb{C}^n . Denote them as $\{|u_{x,i}\rangle\}_{i=1,2,\dots,n}$, then

$$U_x J = \left(\sqrt{\lambda_1} |u_{x,1}\rangle, \sqrt{\lambda_2} |u_{x,2}\rangle, \dots, \sqrt{\lambda_{N_s}} |u_{x,N_s}\rangle, 0, \dots, 0 \right) \quad (6)$$

and similarly

$$V_x J = \left(\sqrt{\lambda_1} |v_{x,1}\rangle, \sqrt{\lambda_2} |v_{x,2}\rangle, \dots, \sqrt{\lambda_{N_s}} |v_{x,N_s}\rangle, 0, \dots, 0 \right) \quad (7)$$

then (4) becomes

$$const = U_x J (V_x J)^T = \sum_{i=1}^{N_s} \lambda_i |u_{x,i}\rangle \langle v_{x,i}|^* \quad (8)$$

similarly for $y \neq x, y \in M$

$$const = U_y J (V_y J)^T = \sum_{i=1}^{N_s} \lambda_i |u_{y,i}\rangle \langle v_{y,i}|^* \quad (9)$$

Eq(8) and Eq(9) has equal constant on their left side, therefore

$$\sum_{i=1}^{N_s} \lambda_i |u_{x,i}\rangle \langle v_{x,i}|^* = \sum_{i=1}^{N_s} \lambda_i |u_{y,i}\rangle \langle v_{y,i}|^*$$

then

$$\begin{aligned} \lambda_j |u_{x,j}\rangle &= \sum_{i=1}^{N_s} \lambda_i |u_{y,i}\rangle \langle v_{y,i}|^* |v_{x,j}\rangle^* \\ &= \sum_{i=1}^{N_s} \lambda_i \langle v_{x,j} | v_{y,i} \rangle |u_{y,i}\rangle \end{aligned}$$

so

$$|u_{x,j}\rangle = \sum_{i=1}^{N_s} \frac{\lambda_i}{\lambda_j} \langle v_{x,j} | v_{y,i} \rangle |u_{y,i}\rangle \quad (10)$$

which shows that the left N_s columns of U_x are linear combinations of left N_s columns in another U_y . Because x, y are arbitrarily chosen messages from M , the left N_s columns of all $U_x \in \{U_i\}_{i \in M}$ span the same linear space \mathbb{C}^{N_s} . Similar statement also holds for $\{V_i\}_{i \in M}$.

Now rewrite Eq(5) according to Eq(7)

$$\begin{aligned} P_{wce} &= \min_{|V|=m} \max_{V_x, V_y \in V, V_x \neq V_y} \left| \sum_{i=1}^{N_s} \lambda_i^2 \langle v_{x,i} | v_{y,i} \rangle \right|^2 \\ &= \min_{|V|=m} \max_{V_x, V_y \in V, V_x \neq V_y} \left| \text{tr} \left(\sum_{i=1}^{N_s} \lambda_i |v_{x,i}\rangle \langle i| \left(\sum_{i=1}^{N_s} \lambda_i |v_{y,i}\rangle \langle i| \right)^\dagger \right) \right|^2 \\ &= \min_{|V|=m} \max_{V_x, V_y \in V, V_x \neq V_y} \left| \text{tr} \left(\left(\sum_{i=1}^{N_s} \lambda_i |v_{y,i}\rangle \langle i| \right)^\dagger \sum_{i=1}^{N_s} \lambda_i |v_{x,i}\rangle \langle i| \right) \right|^2 \end{aligned}$$

Let $Q_x = \sum_{i=1}^{N_s} \lambda_i |v_{x,i}\rangle\langle i|$, $Q_y = \sum_{i=1}^{N_s} \lambda_i |v_{y,i}\rangle\langle i|$, the above equation is equivalent to

$$P_{wce} = \min_{|V|=m} \max_{V_x, V_y \in V, V_x \neq V_y} |tr(Q_y^\dagger Q_x)|^2$$

Note that Q_x, Q_y are both linear operators on \mathbb{C}^{N_s} , according to Lemma (1) and Welch Bound we have

$$P_{wce} \geq \frac{m - N_s^2}{N_s^2(m - 1)}$$

which proves the $N_s < n$ case of Theorem 2.

□

5 Conclusion

This paper discusses the relation between Alice's and Bob's unitary operators in the model of quantum fingerprinting with shared entanglement, and gives a lower bound on the worst case error probability which profiles the ability of this fingerprinting model. In this lower bound, however, quantity of entanglement is measured by Schmidt number. Future work includes the lower bound based on Schmidt coefficients of shared entanglement.

Moreover, Roger's POVM is restrict to be the form $\{|\alpha\rangle\langle\alpha|, I - |\alpha\rangle\langle\alpha|\}$, lower bound with more general POVM is also an open question.

References

- [1] E. Kushilevitz and N. Nisan. *Communication Complexity*. Cambridge University Press, 1997.
- [2] A. C.-C. Yao. Some complexity questions related to distributive computing. *Proceedings of 11th ACM STOC*, pages 209–213, 1979.
- [3] H. Buhrman, R. Cleve, J. Watrous, R. de Wolf. Quantum fingerprinting. *Phys. Rev. Letter*, 87, 2001.
- [4] A. Ambainis. Communication complexity in 3-computer model. *Algorithmica*, 16:298–301, 1996.
- [5] A. J. Scott, J. Walgate, B. C. Sanders. Optimal fingerprinting strategies with one-sided error. *arXiv:quant-ph/0507048*, 2005.

- [6] Rolf T. Horn, A. J. Scott, Jonathan Walgate, Richard Cleve, A. I. Lvovsky, and Barry C. Sanders. Classical and quantum fingerprinting with shared randomness and one-sided error. *arXiv:quant-ph/0501021* v2, 2005.
- [7] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [8] L. R. Welch. Lower bounds on the maximum cross correlation of signals. *IEEE Trans. Inf. Theory*, 20:397, 1974.